CREACIÓN DE HERRAMIENTAS DE SOFTWARE PARA LA CONSTRUCCIÓN DE SISTEMAS DE IOT ESCALABLES Y SEGUROS

Sebastián U. Flores, Mario Berón, Daniel Riesco, Pedro Rangel Henriques
Departamento de Informática - Facultad de Ciencias Físico Matemáticas y Naturales
Universidad Nacional de San Luis - Ejército de Los Andes 950 - San Luis - Argentina
Universidade do Minho Braga - Portugal
s.flores@outlook.com.ar, { mberon, driesco }@unsl.edu.ar
pedrorangelhenriques@gmail.com

RESUMEN

En la actualidad, los avances en el dominio del Internet of Things están transformando las formas en que las personas interactúan con el entorno y están dotando de inteligencia al mismo. Estos progresos buscan mejorar la calidad de vida de las personas, optimizar los procesos industriales e incrementar el cuidado del medio ambiente y de sus recursos. Grandes empresas han implementado modelos de producción innovadores incluyendo dispositivos IoT en sus sistemas, con el fin de incrementar su competitividad de cara a la industria 4.0. Sin embargo, el correcto desarrollo de un sistema de IoT podría ser un desafío si no se toman ciertos recaudos. Uno de los problemas que se presentan, desde la planificación del sistema, es el diseño de una arquitectura que favorezca la escalabilidad en cuanto a cantidad y variedad de dispositivos y usuarios conectados al mismo tiempo, publicando y recibiendo información, garantizando estabilidad, fluidez y seguridad en sus comunicaciones.

En este artículo, se presenta una línea de investigación que aborda la *creación de herramientas de software para la construcción de sistemas de IoT escalables y seguros*, buscando superar las dificultades mencionadas.

Palabras clave: *Sistema de IoT, Dispositivo, Cosa, Escalabilidad, Seguridad, Privacidad, Arquitectura, Internet.*

CONTEXTO

La presente línea de investigación se enmarca en dos Proyectos de Investigación. El primero: "*Ingeniería de Software: Conceptos, Prácticas y Herramientas para el desarrollo de Software con Calidad*" – Facultad de Ciencias Físico- Matemáticas y Naturales, Universidad Nacional de San Luis. Proyecto N.° P-031516. Tal proyecto es la continuación de diferentes proyectos de investigación, a través de los cuales se ha logrado un importante vínculo con distintas universidades a nivel nacional e internacional. Además, se encuentra reconocido por el Programa de Incentivos. El segundo proyecto: "*Fortalecimiento de la Seguridad de los Sistemas de Software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa*" realizado en conjunto con la Universidade do Minho Braga, Portugal, fue aprobado por el Ministerio de Ciencia, Tecnología e Innovación Productiva (MinCyT), y su código es PO/16/93.

1. INTRODUCCIÓN

El término IoT es la abreviación de la frase en inglés "Internet of Things" (i.e. Internet de las Cosas). El mismo corresponde a un dominio de aplicación que integra diferentes campos tecnológicos y sociales. De acuerdo

con IEEE et. al. [1], aún no se ha alcanzado un consenso en cuanto a una definición del mismo, que contenga todas sus características y pueda facilitar una mejor comprensión de su alcance.
Existen varios puntos importantes a destacar en el Software de los sistemas de IoT [1]:

- Los sistemas operativos usados en dispositivos IoT deben estar diseñados para ejecutarse de forma eficiente (ya que trabajan en componentes de pequeña escala), sin dejar de proporcionar funcionalidades básicas que den soporte a los objetivos y propósitos de las aplicaciones ejecutadas en ellos [2][3][4].

- Al contar con escaso almacenamiento y con una capacidad de procesamiento reducida, es muy importante el desarrollo de interfaces de programación de aplicaciones (APIs) que favorezcan la reutilización de componentes y una adecuada gestión de los datos a almacenar/procesar[2][5][6][7].

- Los sistemas de IoT, potencialmente pueden crecer y llegar a componerse por millones de dispositivos diferentes, cada uno ubicado en lugares remotos del planeta y con usuarios ubicados también remotamente. En este contexto, la autogestión y auto-optimización de cada dispositivo y/o subsistema individual podría convertirse en la norma [2][3][8].

- La privacidad y seguridad deben ser garantizadas en cada proceso de los sistemas de IoT, ya que los mismos producen y manejan información reservada [7][9][10][11].

- Para garantizar la escalabilidad de un sistema de IoT, este debe poseer un diseño arquitectónico adecuado. Por la característica previamente mencionada, se entiende la creación de un sistema flexible que permita interconectar tantos dispositivos IoT como sea necesario. Tal interconexión se realiza sin que importe el medio de conexión físico o el sistema operativo que posea cada uno de ellos, siempre y cuando utilicen las interfaces de software y protocolos de comunicación adecuados [12][13][2][8].

- Finalmente, dado los sistemas de IoT manipulan información sensible de personas y organizaciones, deben ser concebidos y conducidos dentro de las restricciones y regulaciones de cada país.

Más allá de las características particulares de cada uno, los sistemas de IoT pueden ser utilizados en los siguientes ámbitos:

- Sistemas de domótica.

- Extracción y análisis automáticos o semi-automáticos de datos en líneas de producción industrial, que permitan optimizar los procesos de negocio [14].

- Monitoreo del estado físico de personas o animales, o extensión de sus capacidades físicas, a través de dispositivos que puedan ser vestidos.

- Monitoreo de cultivos, riego inteligente y control remoto de maquinaria utilizada en la industria agropecuaria (e.g. cosechadoras automáticas).

- Monitoreo del estado del medio ambiente, para la creación de ciudades inteligentes, el control del impacto en la naturaleza de la extracción de recursos naturales y la construcción de una industria más ecológica en general.

Los sistemas de IoT no necesariamente requieren de interacción humana en sus procesos. ETSI [12] trata los sitemas de IoT autónomos y semi-autónomos al definir las comunicaciones "*Machine-to-Machine (M2M)*" (en español, comunicaciones Máquina a Máquina), como aquellas realizadas directamente entre dispositivos y/o subsistemas de IoT,

con interacción humana escasa o nula. Esta clase de comunicaciones posee varias aplicaciones:

- Automatización de actividades repetitivas y/o de carácter determinístico, en las cuales los avances tecnológicos nos permiten prescindir de intervención humana.
- Aprendizaje de patrones de comportamiento humano o patrones en el funcionamiento de procesos propios del sistema. En este caso, la única interacción humana que podría presentarse es la de supervisión de los resultados del aprendizaje realizado por el sistema.
- Autonomización de un sistema aislado, localizado en una ubicación de difícil acceso para las personas.
- Edificios inteligentes que se adapten automáticamente a las condiciones del entorno. En este caso, existiría una constante comunicación entre subsistemas de IoT distribuidos en todo el edificio y sus alrededores, cada uno evaluando las condiciones de su propio entorno y comunicando los cambios relevantes al resto de los subsistemas, para que cada uno se adapte de la mejor forma.

Por lo mencionado en los párrafos anteriores, se puede notar que es difícil la creación de un marco general de trabajo que permita desarrollar e integrar sistemas de IoT de diversa escala y con ámbitos de aplicación heterogéneos. Este marco debe ser lo suficientemente flexible para permitir modificaciones estructurales de los sistemas, de una forma comprensible y segura. También, debe permitir la obtención de múltiples vistas que representen diferentes propiedades de los mismos. Para crear este marco de trabajo, es necesario detectar y comprender los problemas a los que se enfrentan los arquitectos y desarrolladores de sistemas de IoT y que, de acuerdo con Kranz et al. [14], llevan a que un 60 % de las iniciativas IoT se estanquen en la fase de prueba de concepto y, del 40 % restante, sólo el 26 % sean consideradas un completo éxito. Para concluir esta introducción, es importante mencionar que se prevé un amplio crecimiento en la cantidad de objetos conectados a internet a través de sistemas de IoT. De hecho, Kranz et al. estima que, durante el año 2020, se alcanzará una cifra de 50.000 millones de objetos conectados en todo el mundo [14].

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

En la actualidad, existe una gran variedad de sistemas operativos destinados a dispositivos IoT (e.g. TinyOS, Raspbian, RIOT, Ubuntu, Windows 10 IoT Core) [1][4]. También, existe una gran cantidad de librerías y aplicaciones implementadas con el fin de brindar soporte a desarrolladores de sistemas de IoT.
De acuerdo con IEEE et. al. [1], frente al crecimiento en la cantidad de *cosas conectadas a internet*, cada una perteneciendo posiblemente a diferentes *dominios de administración* (i.e. diferentes sistemas/subsistemas de IoT), es necesario repensar por completo los enfoques tradicionales en el desarrollo de aplicaciones web, siendo prioritarios elementos como la escalabilidad y la lógica distribuida.
Por otro lado, mientras que el IoT promete una mejor vida a través de dispositivos conectados y de la información que ellos generen, también marca el comienzo de una nueva era en cuanto a la privacidad y la seguridad. OWASP lista los 10 principales problemas de seguridad que suelen presentarse en sistemas de IoT de toda índole [15].
Frente a lo mencionado en los párrafos anteriores, está claro que los desarrolladores de sistemas de IoT se enfrentan a un problema principal: *la creación de herramientas de software para la construcción de sistemas de IoT escalables y seguros.*
Esta línea de investigación propone:

- Investigar en profundidad las vulnerabilidades de seguridad que afectan a los

sistemas de IoT.

- Investigar el estado del arte de los patrones/estilos arquitectónicos de sistemas de IoT, y de los protocolos utilizados en su desarrollo.

- Integrar las investigaciones realizadas con el fin de crear un conjunto de herramientas que faciliten al desarrollador la creación de sistemas de IoT escalables y seguros, brindando soporte en la integración de subsistemas que posiblemente estén ubicados en diferentes posiciones geográficas, posean diferentes sistemas operativos y utilicen diferentes protocolos de software y hardware.

3. RESULTADOS OBTENIDOS/ESPERADOS

Con el objetivo de evaluar los conceptos investigados, se implementaron dos herramientas de software. La primera de ellas es F-IoT Core [16], una aplicación backend desarrollada en el framework Grails [17] que nuclea toda la lógica de negocio de F-IoT y expone APIs REST para la configuración y monitoreo de sistemas de IoT de diferentes formas. Con el fin de desarrollar un Frontend para acceder de forma más amigable a las configuraciones de los sistemas de IoT gestionados por F-IoT Core, se incorporó la segunda herramienta llamada F-IoT Frontend. La misma consiste en una aplicación web implementada en el framework Angular 8 [18], que brinda al usuario una vista de todos los sistemas de IoT registrados y le permite tanto modificarlos estructuralmente, como visualizar el último estado reportado de los dispositivos que lo comprenden.
A futuro se poseen los siguientes objetivos:

- Implementar en F-IoT Frontend un sistema de visualización en tiempo real del estado de los dispositivos IoT, a través de sistemas del estado del arte. Actualmente se está incursionando en el uso de sockets Web, a través de la librería Socket.IO [19], una de las más usadas por los desarrolladores Web en el mundo, dado que posee una gran flexibilidad y robustez, mucha documentación, es gratuita y de código abierto.

- Realizar una investigación profunda acerca de las amenazas de seguridad que afectan a los sistemas de IoT, y crear una capa de seguridad que abarque todas las comunicaciones realizadas en F-IoT.

- Crear patrones de diseño arquitectónico que puedan ser usados en diferentes ámbitos de aplicación de sistemas de IoT e indicar, para cada patrón, aquellos ámbitos en los que sea más viable su implementación.

- Analizar y comparar las diferentes tecnologías IoT disponibles para ejecución en la Nube, a través de servicios provistos por terceros (e.g. Microsoft, Google, Amazon, IBM, Oracle).

4. FORMACIÓN DE RECURSOS HUMANOS

Los progresos obtenidos en esta línea de investigación sirven como base para el desarrollo de tesis de posgrado, ya sea de doctorado o maestrías en Ingeniería de Software y desarrollo de trabajos finales de las carreras Licenciatura en Ciencias de la Computación, Ingeniería en Informática e Ingeniería en Computación de la Universidad Nacional de San Luis, en el marco de los Proyectos de Investigación mencionados en la Sección *Contexto*.

5. BIBLIOGRAFÍA

[1] IEEE. (mayo de 2015). Towards a Definition of the Internet of Things(IoT), dirección: `https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf`. Último acceso: 01 03 2020.

[2] IETF. (2010). The Internet of Things - Concept and Problem Statement, dirección: https://www.ietf.org/archive/id/draft-lee-iot-problem-statement-05.txt.

[3] CERP-IoT. (2010). Visions and Challenges for Realising the Internet of Things, dirección: http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf.

[4] S. Pérez, P. Gaur y M. P. Tahiliani, «Operating Systemas for IoT Devices: A Criical Survey», *IEEE Region 10 Symposium*, mayo de 2015.

[5] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange y S. Messner, «Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model», *SpringerOpen*, 2013.

[6] H. Ren, H. Li, Y. Dai, K. Yang y X. Lin. (mar. de 2018). Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities, dirección: http://ieeexplore.ieee.org/document/8315210/.

[7] T. Choudhury, A. Gupta, S. Pradhan, P. Kumar e Y. S. Rathore. (oct. de 2017). Privacy and Security of Cloud-Based Internet of Things (IoT), dirección: http://ieeexplore.ieee.org/document/8307328/.

[8] A. Zanella, N. Buis, A. Castellani, L.Vangelista y M. Zorzi, «Internet of Things for Smart Cities», *IEEE Internet of Things Journal*, feb. de 2014.

[9] M. El-hajj, M. Chamoun y F. S. Ahmed. (dic. de 2017). Taxonomy of authentication techniques in Internet of Things (IoT), dirección: http://ieeexplore.ieee.org/document/8305419/.

[10] J. Singh, T. Pasquier, J. Bacon, H. Ko y D. Eyers, «Twenty Security Considerations for Cloud-Supported Internet of Things», *IEEE Internet of Things Journal*, 2015.

[11] S. Pérez, J. L. Hernández-Ramos, S. N. Matheu-García, D. Rotondi, A. F. Skarmeta, L. Straniero y D. Pedone. (feb. de 2018). A lightweight and flexible encryption scheme to protect sensitive data in Smart Building scenarios, dirección: http://ieeexplore.ieee.org/document/8279412/.

[12] ETSI. (sep. de 2010). ETSI Technical Specification, Machine-to-Machine Communications (M2M); M2M Service Requirements. Technical Specification. ver. 1.1.1, dirección: www.etsi.org/deliver/etsi_ts/102600_102699/102689/01.01.01_60/ts_102689v010101p.pdf.

[13] D. Zeng, S. Guo y Z. Cheng. (2011). Journal of Communicaitons, dirección: http://www.jocm.us/index.php?m=content&c=index&a=show&catid=50&id=134.

[14] M. Kranz, *Internet Of Things. Construye nuevos modelos de negocio.* LID Editorial, 2017, ISBN: 9788416894895.

[15] OWASP. (2018). Project Internet of Things, dirección: https://owasp.org/www-project-internet-of-things/.

[16] S. Flores, M. Berón, D. Riesco, P. Henriques y M. Bustos, «F-IoT Core, una Herramienta para el Desarrollo de Soluciones IoT Escalables y Flexibles», *CoNaIISI*, 2018.

[17] I. Object Computing. (2020). Grails Framework, dirección: https://grails.org/.

[18] Google. (2020). Angular Framework, dirección: https://angular.io/.

[19] S. IO. (2020). Socket.IO, dirección: https://socket.io/.